PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-219853
(43)Date of publication of application : 18.08.1995

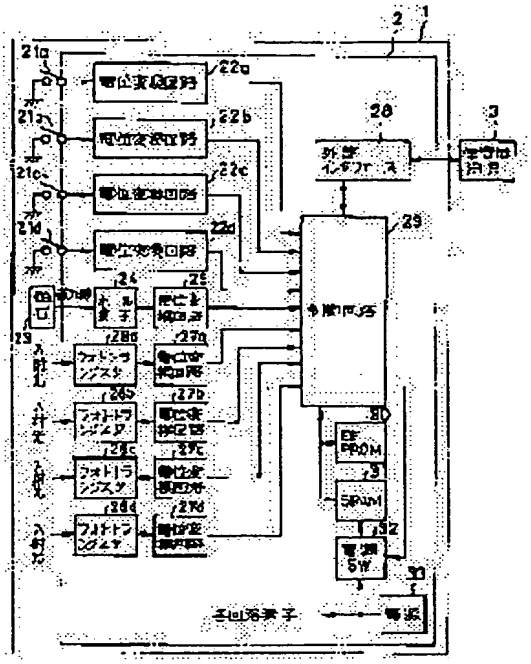
(51)Int.CI. G06F 12/14

(21)Application number : 06-008199
(22)Date of filing : 28.01.1994

(71)Applicant : NEC ENG LTD
(72)Inventor : SAKAKIBARA OSAMU

(54) TERMINAL EQUIPMENT

(57)Abstract:
PURPOSE: To recognize an illicit access without using any mechanical means.
CONSTITUTION: The spring-shaped metallic parts 21a-21d and the potential converting circuits 22a-22d are provided on a printed circuit board 2 and electrically detect the dismantling of a terminal equipment 1. Meanwhile a magnet 23, a Hall element 24 and a potential converting circuit 25 which are attached to a housing magnetically detect the dismantling of the equipment 1. Furthermore the phototransistors 26a-26d and the potential converting circuits 27a-27d optically detect the dismantling of the equipment 1 respectively. A control circuit 29 decides whether the reasons of notifications are due to the accidental troubles such as the falls, etc., or the illicit dismantling done by a malicious third party based on the order and combinations of notifications given from the circuits 22a-22d, 25 and 27a-27d. If the illicit dismantling is decided, the circuit 29 erases the secret information stored in an EEPROM 30 and an SRAM 31. Then the circuit 29 cirtificates a maintenance jig 3 with each other through an external interface 28.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－219853

(43)公開日　平成７年(1995)８月18日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/14	３２０　Ｄ			

審査請求　未請求　請求項の数４　ＯＬ　（全 11 頁）

(21)出願番号　特願平6－8199

(22)出願日　平成６年(1994)１月28日

(71)出願人　000232047
日本電気エンジニアリング株式会社
東京都港区芝浦三丁目18番21号

(72)発明者　榊原　修
東京都港区西新橋三丁目20番４号　日本電気エンジニアリング株式会社内

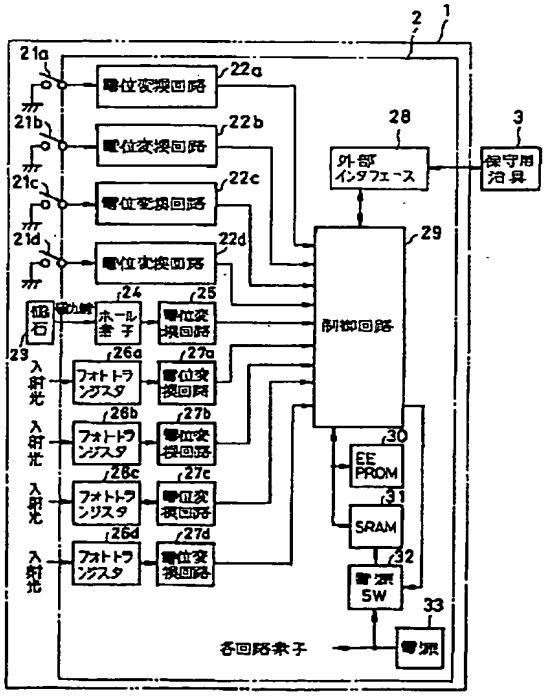
(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　端末装置

(57)【要約】

【目的】　機械的な手段を用いることなく、不正アクセスの認識を可能とする。

【構成】　プリント配線基板２上のバネ状の金具２１ａ～２１ｄ及び電位変換回路２２ａ～２２ｄは端末装置１の解体を電気的に検出する。筐体に取付けた磁石２３とホール素子２４と電位変換回路２５とは端末装置１の解体を磁気的に検出する。フォトトランジスタ２６ａ～２６ｄと電位変換回路２７ａ～２７ｄとは端末装置１の解体を光学的に検出する。制御回路２９は電位変換回路２２ａ～２２ｄ，２５，２７ａ～２７ｄからの通知の順序及び組合せ等によって通知原因を落下等の偶発事故によるものか悪意の第三者の不正解体によるものかを判断する。制御回路２９は悪意の第三者の不正解体によるものと判断すると、ＥＥＰＲＯＭ３０及びＳＲＡＭ３１に記憶された秘密情報を消去する。制御回路２９は外部インタフェース２８を通じて保守用治具３との間で相手認証を行う。



1

【特許請求の範囲】

【請求項１】　秘密情報を記憶するメモリを含む電子回路が搭載されたプリント配線基板と、前記プリント配線基板を収納する外部筐体と、前記電子回路に対する外部からのアクセス許可要求の適否を判定する判定手段と、前記外部筐体の解体の有無を検出する複数の検出手段と、前記判定手段の判定結果及び前記複数の検出手段各々の検出結果に基づいて前記外部筐体の不正な解体か否かを判断する判断手段と、前記判断手段が前記外部筐体の不正な解体と判断したときに前記秘密情報を前記メモリから消去する手段とを含むことを特徴とする端末装置。

【請求項２】　前記判定手段は、相手認証方式によって前記アクセス許可要求の適否を判定するよう構成されたことを特徴とする請求項１記載の端末装置。

【請求項３】　前記複数の検出手段は、前記外部筐体の解体を電気的に検出する第一の検出手段と、前記外部筐体の解体を光学的に検出する第二の検出手段と、前記外部筐体の解体を磁気的に検出する第三の検出手段とを含むことを特徴とする請求項１または請求項２記載の端末装置。

【請求項４】　前記判断手段は、前記判定手段が前記アクセス許可要求なし及び前記アクセス許可信号の否のうち一方を検出したときに前記第一の検出手段と前記第二の検出手段と前記第三の検出手段とにおける夫々の検出状態及びその順序に応じて前記外部筐体の不正な解体か否かを判断するよう構成されたことを特徴とする請求項３記載の端末装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は端末装置に関し、特に移動体通信端末装置の秘匿情報漏洩防止方式に関する。

【０００２】

【従来の技術】従来、この種の秘匿情報漏洩防止方式においては、装置筐体が不正に破壊もしくは解体され、内部の電子回路内のメモリに記憶されている秘密情報が不正に取出されるのを防止するために、装置筐体が不正に破壊もしくは解体されるのを検知したときにメモリ内の秘密情報を消去するよう構成されている。

【０００３】すなわち、図７に示すように、通常、錠４５が取付けられている装置筐体の扉（図示せず）及び錠４５に夫々取付けられた柱状突起４１，４６がマイクロスイッチ４３，４８のバネ板４２，４７を押圧することで、マイクロスイッチ４３，４８がオン状態となっている。

【０００４】内部の電子回路にアクセスする場合に錠４５を開錠すると、柱状突起４６が上方に離れてマイクロスイッチ４８のバネ板４７が解放され、マイクロスイッチ４８がオフ状態となる。アクセス開始検出回路４９はマイクロスイッチ４８がオフ状態となったことを検出すると、判定回路５０にアクセス開始信号１０２を出力する。

2

【０００５】この後に、装置筐体の扉を開けると、柱状突起４１が上方に離れてマイクロスイッチ４３のバネ板４２が解放され、マイクロスイッチ４３がオフ状態となる。内部アクセス検出回路４４はマイクロスイッチ４３がオフ状態となったことを検出すると、判定回路５０に内部アクセス信号１０１を出力する。

【０００６】判定回路５０は上述の如く、錠４５が開錠されてから装置筐体の扉が開けられると、アクセス開始検出回路４９からアクセス開始信号１０２が入力された後に内部アクセス検出回路４４から内部アクセス信号１０１が入力されるので、不正アクセス信号１０３を抹消信号発生回路５１に出力しない。よって、抹消信号発生回路５１からメモリ５２に抹消信号１０４が出力されないため、メモリ５２に記憶されている秘密情報が消去されることはない。

【０００７】これに対して、錠４５を開錠することなく、装置筐体の扉が開けられると、内部アクセス検出回路４４から判定回路５０に内部アクセス信号１０１が出力される。

【０００８】判定回路５０はアクセス開始検出回路４９からアクセス開始信号１０２が入力されていないにもかかわらず、内部アクセス検出回路４４から内部アクセス信号１０１が入力されるので、不正アクセスがあったとして不正アクセス信号１０３を抹消信号発生回路５１に出力する。

【０００９】よって、抹消信号発生回路５１からメモリ５２に抹消信号１０４が出力されるので、この抹消信号１０４に応答してメモリ５２に記憶されている秘密情報が消去される。

【００１０】上述した秘匿情報漏洩防止方式の技術については、特公平１－４７０５９号公報に詳述されている。

【００１１】

【発明が解決しようとする課題】上述した従来の秘匿情報漏洩防止方式では、錠やマイクロスイッチ等の機械的な手段を用いて内部の電子回路への不正アクセスを検出しているため、装置筐体の構成材料である金属やプラスチック等に対して可透過の性質を持つＸ線や超音波等を使用し、装置筐体外部から不正アクセスを検出する構造を解析する手段を有する悪意の第三者に対しては不正アクセスを阻止することができない。

【００１２】また、アクセスの正当性確認のために錠やマイクロスイッチ等の機械的な手段を使用するため、装置に対して容積や重量の増大を招く。さらに、一般的に錠と鍵との組合せは１０の４乗程度であるため、不正開錠の恐れが高い。

【００１３】さらにまた、落下事故等によって装置が機械的に破損したり、荷重を受けたときに不正アクセスと

誤認して秘密情報を消去する場合があり、実使用上問題のない軽微な筐体の損傷であっても修理や保守を行わない限り、機器の運用が不可能となる。

【００１４】そこで、本発明の目的は上記の問題点を解消し、機械的な手段を用いることなく、不正アクセスの認識を可能とすることができる端末装置を提供することにある。

【００１５】

【課題を解決するための手段】本発明による端末装置は、秘密情報を記憶するメモリを含む電子回路が搭載されたプリント配線基板と、前記プリント配線基板を収納する外部筐体と、前記電子回路に対する外部からのアクセス許可要求の適否を判定する判定手段と、前記外部筐体の解体の有無を検出する複数の検出手段と、前記判定手段の判定結果及び前記複数の検出手段各々の検出結果に基づいて前記外部筐体の不正な解体か否かを判断する判断手段と、前記判断手段が前記外部筐体の不正な解体と判断したときに前記秘密情報を前記メモリから消去する手段とを備えている。

【００１６】

【実施例】次に、本発明の一実施例について図面を参照して説明する。

【００１７】図１は本発明の一実施例の構成を示すブロック図である。図において、端末装置１内部に載置されたプリント配線基板２には端末装置１の解体を電気的に検出するためのバネ状の金具２１ａ～２１ｄと、端末装置１の解体を磁気的に検出するためのホール素子２４と、端末装置１の解体を光学的に検出するためのフォトトランジスタ２６ａ～２６ｄとが搭載されている。

【００１８】バネ状の金具２１ａ～２１ｄは端末装置１の筐体（図示せず）が組立て状態にあるときにグランドと導通状態となり、筐体が解体されるときにグランド電位とは異なる電位を持つことになる。

【００１９】プリント配線基板２上の電位変換回路２２ａ～２２ｄ各々は対応するバネ状の金具２１ａ～２１ｄの電位変化を検出し、検出／非検出の二値信号に変換して制御回路２９に通知する。

【００２０】ホール素子２４はプリント配線基板２の上面中央に実装され、プリント配線基板２の上面に対向する端末装置１の筐体の内面中央に載置された磁石２３の磁界変化を検出し、その磁界変化を電気信号に変換して出力する。

【００２１】電位変換回路２５はホール素子２４で電気信号に変換された磁界変化を検出し、検出／非検出の二値信号に変換して制御回路２９に通知する。尚、ホール素子２４は磁界指向性がよく、磁界の強さに対して出力値が電位変換回路２５の電源電圧まで飽和しないものが好ましい。

【００２２】これによって、端末装置１の製造時に正規組立状態でのホール素子２４の出力値をＥＥＰＲＯＭ３０に記録することで、その出力値以上の磁界の強さを検出した場合に端末装置１の筐体の解体の可能性があると判断することが可能となる。

【００２３】フォトトランジスタ２６ａ～２６ｄはプリント配線基板２の上面及び下面に夫々２つずつ実装されており、プリント配線基板２の上面及び下面各々の同一面側では上部側及び下部側に振り分けられて実装されている。

【００２４】この場合、同一面側の上部側及び下部側に実装されたフォトトランジスタはその二つの素子の受光感度半値角の延長線がプリント配線基板２と相対する筐体の内壁との間の空間で交わることが望ましい。

【００２５】また、プリント配線基板２の短辺側の端部にフォトトランジスタを搭載する場合に、そのフォトトランジスタの受光感度半値角は９０°に近ければ近いほどよい。

【００２６】フォトトランジスタ２６ａ～２６ｄは端末装置１の筐体が解体されて外部から光線が照射されると、その出力値を変化させる。電位変換回路２７ａ～２７ｄは対応するフォトトランジスタ２６ａ～２６ｄの出力の変化を検出し、検出／非検出の二値信号に変換して制御回路２９に通知する。

【００２７】制御回路２９は電位変換回路２２ａ～２２ｄ，２５，２７ａ～２７ｄからの通知を受けると、それら通知の順序及び組合せ等によって通知原因を落下等の偶発事故によるものか悪意の第三者の不正解体によるものかを判断する。制御回路２９は悪意の第三者の不正解体によるものと判断すると、ＥＥＰＲＯＭ３０及びＳＲＡＭ３１に記憶された秘密情報を消去する。

【００２８】ＥＥＰＲＯＭ３０には秘密情報として、回線網（図示せず）との接続に必要なパラメータ、端末装置使用者の個人データ、保守用治具３の相手認証に必要な情報等が記憶されている。

【００２９】また、ＳＲＡＭ３１には秘密情報として、発呼先登録、受信内容記憶、発呼・着呼等通話記録、課金情報・記録等が記憶されている。

【００３０】ＥＥＰＲＯＭ３０及びＳＲＡＭ３１は制御回路２９に接続され、必要に応じて制御回路２９から書込み及び読出しが行われる。ここで、本発明の一実施例ではＥＥＰＲＯＭ３０及びＳＲＡＭ３１を併記したが、端末装置１の回路構成によってはどちらか一方か、あるいは類似の記憶素子であってもよい。

【００３１】また、制御回路２９は外部インタフェース２８を介して保守用治具３と通信可能となっており、端末装置１の筐体の保守解体時には保守用治具３から端末装置１に対する相手認証が行われる。

【００３２】電源スイッチ（ＳＷ）３２は電源３３からＳＲＡＭ３１に対する電源を制御回路２９からの制御信号に応じてオンオフ制御する。電源３３はＳＲＡＭ３１に対して電源を供給するとともに、プリント配線基板２

5

上の各回路素子に電源を供給する。

【００３３】図２は本発明の一実施例の組立図であり、図３は組立て状態における図２のＡＡ線に沿う矢視方向の断面図であり、図４は組立て状態における図２のＢＢ線に沿う矢視方向の断面図である。

【００３４】これら図１～図４を用いて端末装置１の組立てを順を追って説明する。まず、プリント配線基板２に対して筐体前面部４及び筐体後面部５を固定するためのネジ穴部周辺を除いた端部全周域にベリリウム銅やリン青銅等のバネ性を持った導電性金属からなる金具８ａ～８ｌを嵌め込む。このとき、プリント配線基板２のグランドと金具８ａ～８ｌとは電気的に導通状態となる。

【００３５】また、上記と同様の導電性金属からなるバネ状の金具２１ａ～２１ｄはプリント配線基板２の端部のグランドと導通している銅箔部の上に被さるように、かつ銅箔部に接触しない状態でプリント配線基板２のパターンに半田付けされ、電位変換回路２２ａ～２２ｄの入力に夫々接続される。

【００３６】プリント配線基板２をネジ９ａ，９ｂで筐体後面部５にネジ止めすると、バネ状の金具２１ｂ，２１ｄは夫々筐体後面部５の内面に押し付けられ、プリント配線基板２の銅箔部に接触する。よって、バネ状の金具２１ｂ，２１ｄはプリント配線基板２のグランドと電気的に導通状態となる。

【００３７】また、筐体後面部５の内面は全体的にアルミニウム蒸着によって電気的に導通可能な状態にあるため、ネジ９ａ，９ｂでプリント配線基板２が筐体後面部５にネジ止めされると、プリント配線基板２のグランドと筐体後面部５の内面とは同一電位となる。

【００３８】次に、密閉用ゴムパッキン７を筐体後面部５の筐体前面部４との接合部に嵌め込み、筐体前面部４の上部の爪４ａを筐体後面部５の上部の爪５ａに引掛け、バネ状の金具２１ａ，２１ｃを夫々筐体前面部４の内面によってプリント配線基板２の銅箔部に接触させた状態で、ネジ９ｅ，９ｆによって筐体後面部５を筐体前面部４にネジ止めする。

【００３９】その後に、ネジ９ｃ，９ｄによって筐体後面部５を筐体前面部４にネジ止めする。ここで、筐体前面部４の内面は筐体後面部５の内面と同様にアルミニウム蒸着されているため、プリント配線基板２のグランドと筐体前面部４の内面とは同一電位となる。

【００４０】したがって、筐体後面部５側と同様に、プリント配線基板２のグランドと筐体前面部４及び筐体後面部５の内面とバネ状の金具２１ａ，２１ｃとは同一電位となる。尚、筐体前面部４の内面中央には磁石２３が、プリント配線基板２上のホール素子２４に対向する位置に取付けられている。

【００４１】最後に、筐体後面部５の溝部５ｂ，５ｃに夫々電池ケース６の爪６ａ，６ｂを嵌め込むことによって、プリント配線基板２に電源が供給可能状態となるので、端末装置１が動作可能となる。

6

【００４２】尚、端末装置１が動作すると、ＬＣＤ（図示せず）上に表示されたメッセージ等をＬＣＤカバーガラス１０を通して見ることが可能になるとともに、キートップ１１を介してキー入力を行うことができる。

【００４３】図５は図２の金具８ａを示す斜視図であり、図６は図５のＣＣ線に沿う矢視方向の断面図である。これらの図において、金具８ａはコの字形状となっており、互いに対向する２つの面８ａ－１，８ａ－２と底面８ａ－３とからなっている。

【００４４】金具８ａはプリント配線基板２に嵌め込むために、その開口側の面８ａ－１，８ａ－２の間隔が底面８ａ－３側の面８ａ－１，８ａ－２の間隔よりも狭くなるように、面８ａ－１，８ａ－２はテーパ状に底面８ａ－３につながっている。

【００４５】また、底面８ａ－３側の面８ａ－１，８ａ－２の間隔はプリント配線基板２の厚さと同一となっているため、金具８ａをプリント配線基板２に嵌め込むだけで金具８ａとプリント配線基板２との間の電気的導通を確保することができる。

【００４６】尚、図示していないが、他の金具８ｂ～８ｌも金具８ａと同一形状となっており、金具８ｂ～８ｌをプリント配線基板２に嵌め込むだけで金具８ｂ～８ｌとプリント配線基板２との間の電気的導通を確保することができる。

【００４７】図７は図２のバネ状の金具２１ａの取付け状態を示す斜視図であり、図８は図７のＤＤ線に沿う矢視方向の断面図である。これらの図において、バネ状の金具２１ａはプリント配線基板２上に載置され、その一端がプリント配線基板２の挿入部品半田付け用導通貫通穴１３に半田付けされている。

【００４８】また、バネ状の金具２１ａは折曲げ部分ａで、その他端がプリント配線基板２上の銅箔部１２に接触しないように折曲げられている。バネ状の金具２１ａの他端は筐体後面部５がネジ９ｃ～９ｆによって筐体前面部４にネジ止めされると、筐体前面部４の内面によってプリント配線基板２上の銅箔部１２に押付けられ、プリント配線基板２のグランドと電気的に導通状態となる。

【００４９】尚、図示していないが、バネ状の金具２１ｂ～２１ｄも上記のバネ状の金具２１ａと同様に、一端がプリント配線基板２の挿入部品半田付け用導通貫通穴１３に半田付けされ、かつ他端がプリント配線基板２上の銅箔部１２に接触しないように折曲げ部分ａで折曲げられている。

【００５０】図９は図１の磁石２３及びホール素子２４による端末装置１の解体の磁気的な検出動作を示す図である。図９（ａ）はプリント配線基板２と筐体前面部４と筐体後面部５とを組立てる前の状態を示しており、図９（ｂ）はプリント配線基板２と筐体前面部４と筐体後

面部５とを組立てた後の状態を示している。

【００５１】これらの図において、磁石２３及びホール素子２４は互いに対向するように、夫々筐体前面部４の内面中央及びプリント配線基板２の上面中央に設置されている。尚、磁石２３は筐体前面部４の内面に取付けられたキースイッチ押え板１４に当接して設置されている。

【００５２】プリント配線基板２と筐体前面部４と筐体後面部５とを組立てると、磁石２３及びホール素子２４は常に当接あるいは接近した状態となり、ホール素子２４は磁石２３の磁界を検出し、一定の信号を出力する。

【００５３】この状態で、端末装置１が解体されると、磁石２３がホール素子２４における磁界検出範囲から外れてしまうので、ホール素子２４は磁石２３の磁界変化を検出し、その磁界変化を電気信号に変換して出力する。これによって、端末装置１の解体を磁気的に検出することが可能となる。

【００５４】図１０は図１のバネ状の金具２１ａ～２１ｄによる端末装置１の解体の電気的な検出動作を示す図である。図１０（ａ）はプリント配線基板２と筐体前面部４と筐体後面部５とを組立てる前の状態を示しており、図１０（ｂ）はプリント配線基板２と筐体前面部４と筐体後面部５とを組立てた後の状態を示している。

【００５５】これらの図において、プリント配線基板２と筐体前面部４と筐体後面部５とを組立てる前にはバネ状の金具２１ａ，２１ｂ各々の他端がプリント配線基板２上の銅箔部１２に接触しないようになっている。

【００５６】プリント配線基板２と筐体前面部４と筐体後面部５とを組立てると、バネ状の金具２１ａ，２１ｂ各々の他端は筐体前面部４及び筐体後面部５の内面によってプリント配線基板２上の銅箔部１２に押付けられ、プリント配線基板２のグランドと電気的に導通状態となる。

【００５７】この状態で、端末装置１が解体され、筐体前面部４及び筐体後面部５がプリント配線基板２から取外されると、バネ状の金具２１ａ，２１ｂ各々の他端がプリント配線基板２上の銅箔部１２から離れるので、バネ状の金具２１ａ，２１ｂの電位が変化する。

【００５８】このバネ状の金具２１ａ，２１ｂの電位変化を検出することで、端末装置１の解体を電気的に検出することが可能となる。

【００５９】図１１は図１の端末装置１における相手認証方法の手順を示すフローチャートである。この図１１を用いて端末装置１における相手認証方法の手順について以下説明する。

【００６０】ここで、ＥＥＰＲＯＭ３０には保守用治具３の相手認証を行うための情報として、端末装置個別番号Ｒ（相手認証方式における検証者側乱数）と、保守用治具識別番号Ｕ（相手認証方式における証明者側乱数）と、相手認証確認用一方向関数ｆ（Ｒ，Ｕ）とが予め格

納されている。

【００６１】また、保守用治具３は相手認証に使用する一方向関数ｆ（Ｒ，Ｕ）を計算機能として有し、相手認証に使用する個別データとして保守用治具識別番号Ｕを有している。

【００６２】まず、保守解体を行う者は保守用治具３の保守用治具識別番号Ｕを図示せぬ記憶部から読出した後に（図１１ステップＳ３１）、外部インタフェース２８を通じて制御回路２９に端末装置個別番号Ｒの送信を要求する（図１１ステップＳ３２）。

【００６３】制御回路２９は予めＥＥＰＲＯＭ３０から端末装置個別番号Ｒを読出しておき（図１１ステップＳ１）、保守用治具３から端末装置個別番号Ｒの送信要求を受信すると（図１１ステップＳ２）、その端末装置個別番号Ｒを保守用治具３に送信する（図１１ステップＳ３）。

【００６４】保守用治具３は制御回路２９から端末装置個別番号Ｒを受信すると（図１１ステップＳ３３）、記憶部から読出した保守用治具識別番号Ｕと制御回路２９から受信した端末装置個別番号Ｒとを一方向関数ｆ（Ｒ，Ｕ）に代入してＭ＝ｆ（Ｒ，Ｕ）を得る（図１１ステップＳ３４）。

【００６５】保守用治具３は算出したＭ＝ｆ（Ｒ，Ｕ）と、記憶部から読出した保守用治具識別番号Ｕとを外部インタフェース２８を通じて制御回路２９に送信する（図１１ステップＳ３５）。

【００６６】制御回路２９は保守用治具３からＭ＝ｆ（Ｒ，Ｕ）と保守用治具識別番号Ｕとを受信すると（図１１ステップＳ４）、ＥＥＰＲＯＭ３０から読出した端末装置個別番号Ｒと、保守用治具３から受信した保守用治具識別番号Ｕとを一方向関数ｆ（Ｒ，Ｕ）に代入してＭ’＝ｆ（Ｒ，Ｕ）を得る（図１１ステップＳ５）。

【００６７】制御回路２９は算出したＭ’＝ｆ（Ｒ，Ｕ）と保守用治具３から受信したＭ＝ｆ（Ｒ，Ｕ）とを比較する（図１１ステップＳ６）。この結果、算出したＭ’＝ｆ（Ｒ，Ｕ）と保守用治具３から受信したＭ＝ｆ（Ｒ，Ｕ）とが異なる値であれば、制御回路２９はそれ以降の通信を止め、拒絶状態に遷移する（図１１ステップＳ７）。

【００６８】また、上記の結果、算出したＭ’＝ｆ（Ｒ，Ｕ）と保守用治具３から受信したＭ＝ｆ（Ｒ，Ｕ）とが等しい値であれば、制御回路２９は保守用治具３を正当な治具と認めてアクノリッジ信号（ＡＣＫ）を保守用治具３に送信する（図１１ステップＳ８）。

【００６９】保守用治具３は制御回路２９からアクノリッジ信号を受信すると（図１１ステップＳ３６）、秘匿情報漏洩防止動作の解除要求を外部インタフェース２８を通じて制御回路２９に送信し（図１１ステップＳ３７）、保守動作を開始する（図１１ステップＳ３８）。

【００７０】制御回路２９は保守用治具３から解除要求

9

を受信すると（図１１ステップＳ９）、秘匿情報漏洩防止動作を解除し（図１１ステップＳ１０）、保守動作の受入れ態勢に入る（図１１ステップＳ１１）。

【００７１】この秘匿情報漏洩防止動作の解除後、上述した端末装置１の解体を電気的に検出する手段と、磁気的に検出する手段と、光学的に検出する手段とが夫々端末装置１の解体を検出しても、ＥＥＰＲＯＭ３０及びＳＲＡＭ３１に記憶された秘密情報は消去されない。

【００７２】尚、上述した相手認証方法については、「高速ディジタル署名方式　ＥＳＩＧＮ」（岡本龍明・藤岡淳・岩田雅彦著、ＮＴＴ　Ｒ&Ｄ　Ｖｏｌ．４０，Ｎｏ．５，１９９１）の第６９４頁右欄下から２行目～第６９５頁右欄６行目記載の「６　相手認証方式」に詳述されている。

【００７３】この例では一方向関数ｆ（Ｒ，Ｕ）として、端末装置個別番号Ｒ及び保守用治具識別番号Ｕ各々の各ビットの排他的論理和演算式が用いられているが、秘密性を高めるためには第三者にわからないような複雑な式を一方向関数ｆ（Ｒ，Ｕ）として用いればよい。

【００７４】上記の図１～図１１を用いて本発明の一実施例の動作について以下説明する。本発明の一実施例においては、端末装置１が認識する解体として保守解体及び不正解体の二種類がある。

【００７５】この二種類の解体の差は保守用治具３が端末装置１で解体を受理している治具かどうかを判断することで決定される。すなわち、端末装置１の解体作業前に保守用治具３からのアクセス要求に対して端末装置１で相手認証を行い、その結果により保守解体か不正解体かが判断される。

【００７６】そこでまず、修理等の目的による保守解体の場合を説明する。端末装置１は製造者から出荷される時点で本発明の一実施例による秘匿情報漏洩防止策が施されている。

【００７７】つまり、端末装置１には上述した端末装置１の解体を電気的に検出する手段と、磁気的に検出する手段と、光学的に検出する手段とが組込まれ、さらに解体を許可する保守用治具３の相手認証を行うための情報がＥＥＰＲＯＭ３０に格納されている。

【００７８】ＥＥＰＲＯＭ３０には保守用治具３の相手認証を行うための情報として、端末装置個別番号Ｒ（相手認証方式における検証者側乱数）と、保守用治具識別番号Ｕ（相手認証方式における証明者側乱数）と、相手認証確認用一方向関数ｆ（Ｒ，Ｕ）とが格納されている。

【００７９】保守解体を行う場合、その保守解体を行うものは予めこれから行われる解体が保守解体であることを端末装置１の制御回路２９に認識させ、秘匿情報漏洩防止動作を解除する必要がある。

【００８０】このため、端末装置１及び保守用治具３には相手認証に使用する一方向関数ｆ（Ｒ，Ｕ）を計算機

10

能として有している。また、相手認証に使用する個別データとして端末装置１は端末装置個別番号Ｒを、保守用治具３は保守用治具識別番号Ｕを夫々有している。

【００８１】上記の番号の桁数や一方向関数式の複雑さによって機械的な錠や電気的な錠に対して１０の１０乗以上高い論理的な施錠効果を得ることが可能となる。

【００８２】まず、保守解体を行う者は保守用治具３を用いて、端末装置１との間で上述した手順で相手認証を行う。これによって、端末装置１の制御回路２９が保守用治具３を正当な治具と認めれば、端末装置１の解体を行ってもＥＥＰＲＯＭ３０及びＳＲＡＭ３１に記憶された秘密情報が消去されることがないので、端末装置１の運用に影響を与えることなく、端末装置１の修理や保守を行うことができる。

【００８３】次に、不正解体の場合を説明する。端末装置１が不正解体と認識するのは事前に相手認証が行われない解体全てである。端末装置１の解体が不正に行われる場合、その手段は正規の解体方法とは限らず、筐体の切断等もあり得る。

【００８４】そこで、本発明の一実施例では電気的、磁気的、光学的の３種類の検出手段によって端末装置１の解体を検出している。以下、上記の３種類の検出手段による検出動作について説明する。

【００８５】端末装置１の解体を電気的に検出する場合について図１０を用いて説明する。不正解体を行う者はプリント配線基板２を露出させ、内部回路動作及びそれに関わるデータを解析することを目的に解体を行うので、筐体前面部４及び筐体後面部５をプリント配線基板２から分離しようとする。

【００８６】このような意図を持って解体が行われる場合、特に筐体の切断等の方法によらなければ、筐体前面部４を筐体後面部５にネジ止めしているネジ９ｃ～９ｆを取外す必要が生ずる。

【００８７】これらのネジ９ｃ～９ｆを取外すと、筐体後面部５にネジ９ａ，９ｂで固定されたプリント配線基板２に半田付けされたバネ状の金具２１ａ，２１ｃによって筐体前面部４がプリント配線基板２から１ｍｍ程度持ち上がる。

【００８８】すると、バネ状の金具２１ａ，２１ｃの他端がプリント配線基板２上の銅箔部１２から離れ、バネ状の金具２１ａ，２１ｃの電位がプリント配線基板２のグランド電位から切離されて異なる電位を持つことになる。

【００８９】電位変換回路２２ａ，２２ｃはバネ状の金具２１ａ，２１ｃの電位変化を検出すると、その検出結果を検出／非検出の二値信号に変換して制御回路２９に通知する。

【００９０】よって、制御回路２９は保守用治具３により秘匿情報漏洩防止動作の解除が行われていないときに、電位変換回路２２ａ，２２ｃからバネ状の金具２１

11

ａ，２１ｃの電位変化を検出が通知されると、ＥＥＰＲＯＭ３０及びＳＲＡＭ３１に記憶された秘密情報を消去する。

【００９１】もちろん、正規の手段によらず、筐体後面部５が筐体前面部４よりも先にプリント配線基板２から分離された場合も、上記の動作と同様にして、端末装置１の解体を検出することはバネ状の金具２１ｂ，２１ｄによって可能である。

【００９２】次に、端末装置１の解体を磁気的に検出する場合について図９を用いて説明する。不正解体を行う者はプリント配線基板２を露出させようとすると、端末装置１の構造上、まず筐体前面部４をプリント配線基板２から分離させなければならない。

【００９３】正規の手段に準じた方法にて端末装置１の解体を行う場合、まず電池パック６を筐体後面部５から取外した後に、筐体後面部５からネジ９ｃ～９ｆを取外す。その後に、筐体前面部４を頭頂部の筐体嵌合用の爪４ａを支点として筐体後面部５から分離させる。

【００９４】そうすると、筐体前面部４内面に取付けた磁石２３がホール素子２４における磁界検出範囲から外れてしまうので、ホール素子２４は磁石２３の磁界変化を検出し、その磁界変化を電気信号に変換して出力する。電位変換回路２５はホール素子２４の出力から磁石２３の磁界変化を検出し、その検出結果を検出／非検出の二値信号に変換して制御回路２９に通知する。

【００９５】よって、制御回路２９は保守用治具３により秘匿情報漏洩防止動作の解除が行われていないときに、電位変換回路２５からホール素子２４による磁石２３の磁界変化の検出が通知されると、ＥＥＰＲＯＭ３０及びＳＲＡＭ３１に記憶された秘密情報を消去する。

【００９６】また、端末装置１の解体を光学的に検出する場合について図１～図４を用いて説明する。不正解体を行う者はプリント配線基板２を露出させようとすると、端末装置１の構造上、筐体前面部４または筐体後面部５をプリント配線基板２から分離させなければならない。

【００９７】正規の手段に準じた方法にて端末装置１の解体を行う場合、まず電池パック６を筐体後面部５から取外した後に、筐体後面部５からネジ９ｃ～９ｆを取外す。その後に、筐体前面部４を頭頂部の筐体嵌合用の爪４ａを支点として筐体後面部５から分離させる。

【００９８】そうすると、プリント配線基板２上のフォトトランジスタ２６ａ～２６ｄのうちいずれか（１つでもあるいは複数でもよい）に外部から光線が照射され、光線が照射されたフォトトランジスタ２６ａ～２６ｄの出力が変化する。

【００９９】電位変換回路２７ａ～２７ｄはフォトトランジスタ２６ａ～２６ｄの出力の変化を検出し、その検出結果を検出／非検出の二値信号に変換して制御回路２９に通知する。

12

【０１００】よって、制御回路２９は保守用治具３により秘匿情報漏洩防止動作の解除が行われていないときに、電位変換回路２７ａ～２７ｄからフォトトランジスタ２６ａ～２６ｄの出力の変化が通知されると、ＥＥＰＲＯＭ３０及びＳＲＡＭ３１に記憶された秘密情報を消去する。

【０１０１】もちろん、正規の手段によらず、筐体後面部５を筐体前面部４よりも先にプリント配線基板２から分離した場合や筐体前面部４または筐体後面部５の一部を切取ったりあるいは切断した場合も、上記の動作と同様にして、端末装置１の解体を検出することはフォトトランジスタ２６ａ～２６ｄによって可能である。

【０１０２】上述した３種類の検出手段によって端末装置１の解体の検出情報は夫々制御回路２９に通知される。制御回路２９は各回路から通知された検出情報の組合せや通知順序等によって通知原因が落下等の偶発的な事故によるものか、あるいは不正解体によるものかを判断区別し、夫々に対応して処理を行う。

【０１０３】これは端末装置１の運用において、落下事故等による衝撃や人もしくは物の下敷きになって荷重を受けることで、筐体の損傷等から不正解体と誤認識し、誤ってＥＥＰＲＯＭ３０及びＳＲＡＭ３１に記憶された秘密情報を消去しないようにするためである。この判断を行うことで、偶発的な事故等による筐体の破損を検出することが可能となる。

【０１０４】制御回路２９が導き出す判断結果として偶発的な事故等による破損と判断した場合、上記３種類の検出手段からの検出情報によって、「運用可能及び加入者に対して修理要求」あるいは「運用不可（ＥＥＰＲＯＭ３０の記憶情報消去）」のうちいずれかの処理を実行する。

【０１０５】これは回線網の立場あるいは加入者の立場から見て、筐体が破損した端末装置１の運用が他に悪影響を与える危険があるので、制御回路２９はこのような対応を実行する。

【０１０６】また、制御回路２９は導き出す判断結果として不正解体による破損と判断した場合、「運用不可（ＥＥＰＲＯＭ３０及びＳＲＡＭ３１の記憶情報消去）」の処理を実行する。

【０１０７】このように、バネ状の金具２１ａ～２１ｄや筐体前面部４及び筐体後面部５の内面の蒸着膜の仲立ちで、筐体とプリント配線基板２とが電気的に同一電位であること、言い換えれば正規な状態で接触していることを検出することによって、プリント配線基板２上の各電子回路への不正なアクセスを認識することが可能となるため、不正アクセス検出専用の機械的あるいは電気的な機構を使用せずに、不正アクセスを認識することができる。

【０１０８】また、不正アクセスの電気的な検出信号や光学的な検出信号、及び磁気的な検出信号を組合せて用

13

いることで、筐体の破壊や解体が故意か事故かを判別し、軽微な機構的損傷であればＥＥＰＲＯＭ３０やＳＲＡＭ３１の秘密情報を保持して端末装置１の運用を可能としながら、使用者に対して修理要求をすることができる。

【０１０９】一方、筐体の破壊や解体が悪意の第三者による不正なアクセスと判断した場合にはＥＥＰＲＯＭ３０やＳＲＡＭ３１の秘密情報を消去し、以後の端末装置１の運用を不可能として情報の漏洩を防ぐことができる。

【０１１０】さらに、端末装置１の解体の正当性証明のための相手認証に錠等の機構的な手段を使用せずに、外部インタフェース２８等の通信回路を用いた論理的な相手認証方式を使用することで、軽量小型で、量産や保守の簡便さを実現することができる。これによって、使用上、落下事故が生じる確率が非常に高い移動体通信端末装置に適用することが可能となる。

【０１１１】

【発明の効果】以上説明したように本発明によれば、秘密情報を記憶するメモリを含む電子回路に対する外部からのアクセス許可要求の適否を判定するとともに、この電子回路が搭載されたプリント配線基板を収納する外部筐体の解体の有無を複数の異なる手段で検出し、これらの判定結果及び検出結果に基づいて外部筐体の不正な解体と判断したときに秘密情報をメモリから消去することによって、機械的な手段を用いることなく、不正アクセスの認識を可能とすることができるという効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例の構成を示すブロック図である。

【図２】本発明の一実施例の組立図である。

【図３】組立て状態における図２のＡＡ線に沿う矢視方向の断面図である。

【図４】組立て状態における図２のＢＢ線に沿う矢視方向の断面図である。

【図５】図２の金具を示す斜視図である。

【図６】図５のＣＣ線に沿う矢視方向の断面図である。

14

【図７】図２のバネ状の金具の取付け状態を示す斜視図である。

【図８】図７のＤＤ線に沿う矢視方向の断面図である。

【図９】（ａ）は図２のプリント配線基板と筐体前面部と筐体後面部とを組立てる前の磁石及びホール素子の状態を示す図、（ｂ）は図２のプリント配線基板と筐体前面部と筐体後面部とを組立てた後の磁石及びホール素子の状態を示す図である。

【図１０】（ａ）は図２のプリント配線基板と筐体前面部と筐体後面部とを組立てる前のバネ状の金具の状態を示す図、（ｂ）は図２のプリント配線基板と筐体前面部と筐体後面部とを組立てた後のバネ状の金具の状態を示す図である。

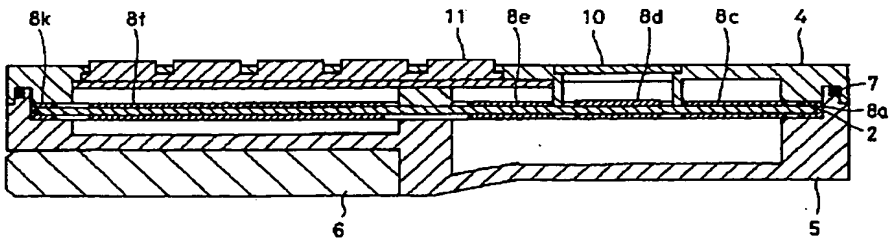
【図１１】図１の端末装置における相手認証方法の手順を示すフローチャートである。

【図１２】従来例の構成を示すブロック図である。

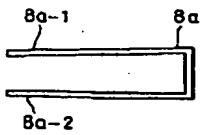
【符号の説明】

１　端末装置
２　プリント配線基板
３　保守用治具
４　筐体前面部
５　筐体後面部
６　電池パッケージ
７　密閉用ゴムパッキン
８ａ～８ｌ　金具
９ａ～９ｆ　ネジ
１２　銅箔部
２１ａ～２１ｄ　バネ状の金具
２２ａ～２２ｄ，２５，２７ａ～２７ｄ　電位変換回路
２３　磁石
２４　ホール素子
２６ａ～２６ｄ　フォトトランジスタ
２８　外部インタフェース
２９　制御回路
３０　ＥＥＰＲＯＭ
３１　ＳＲＡＭ

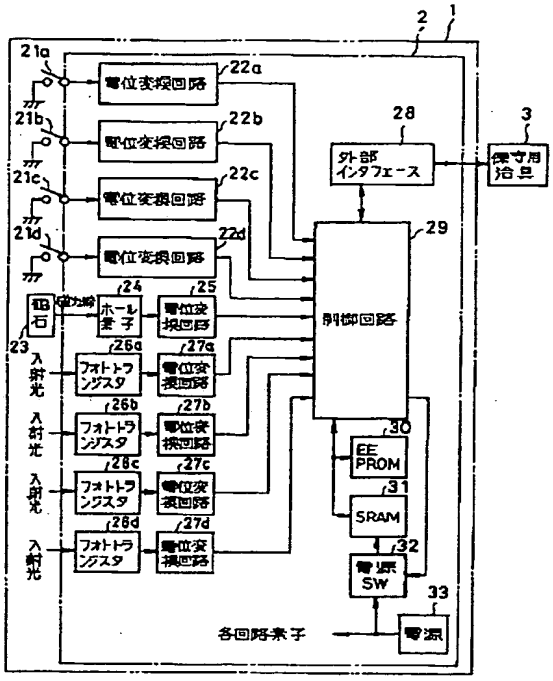
【図３】



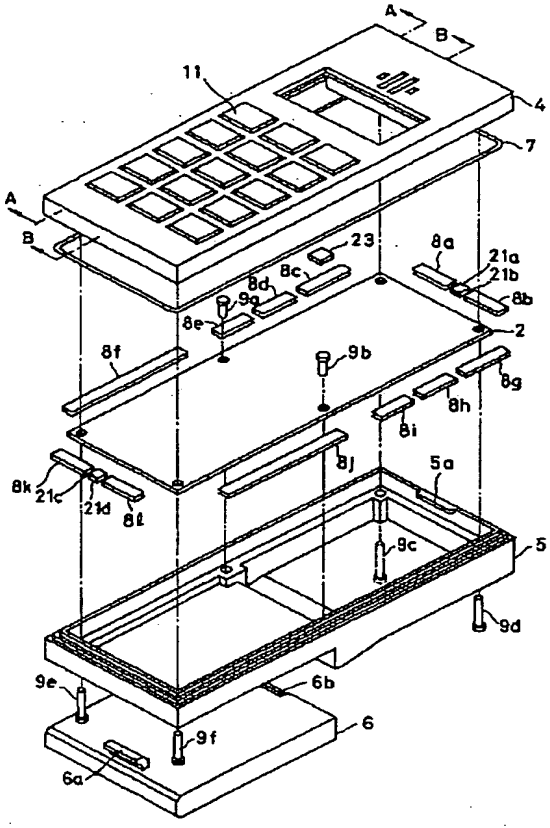
【図６】



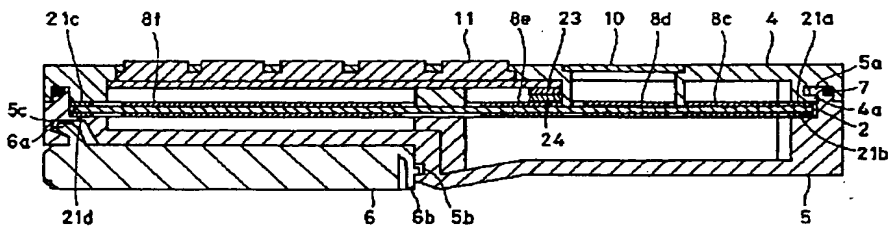
【図１】


2
1
21a
21b
21c
21d
電位変換回路
22a
22b
22c
22d
28
外部インタフェース
3
保守用治具
29
制御回路
磁石
23
ホール素子
24
25
入射光
フォトトランジスタ
26a
26b
26c
26d
27a
27b
27c
27d
EEPROM
30
SRAM
31
電源SW
32
33
電源
各回路素子

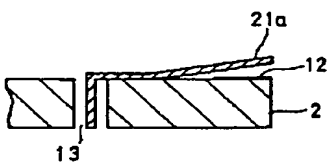
【図２】


A
B
11
4
7
23
8a
21a
21b
8b
8c
8d
9a
8e
2
8f
9b
8g
8h
8i
8j
5a
8k
21c
21d
8l
9c
5
9d
9e
6b
6
9f
6a

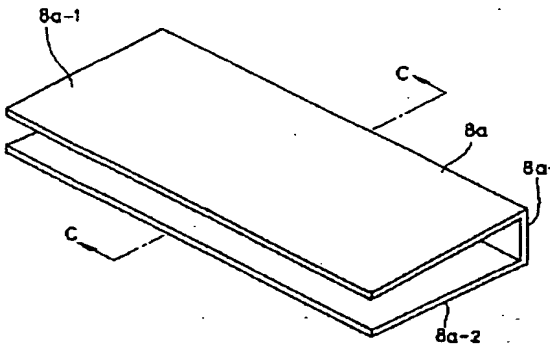
【図４】


21c
8f
11
8e
23
10
8d
8c
4
21a
5a
7
5c
4a
6a
2
24
21b
21d
6
6b
5b
5

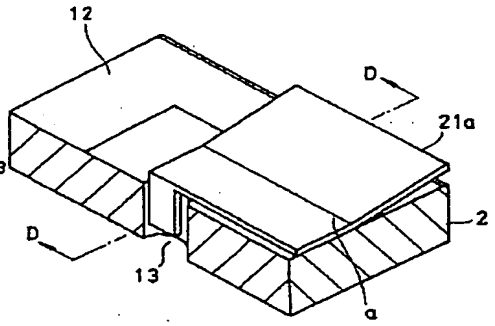
【図８】


21a
12
2
13

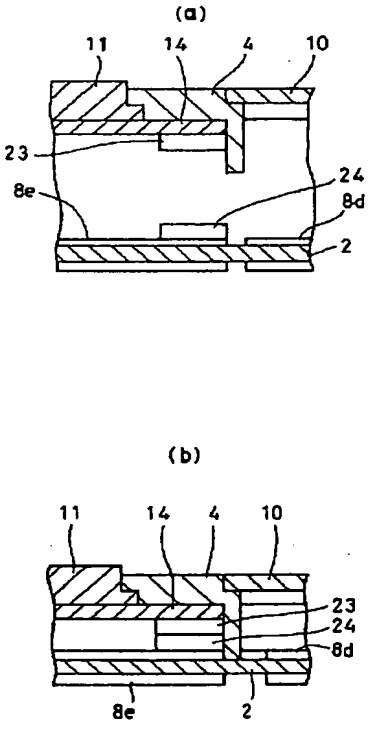
【図5】



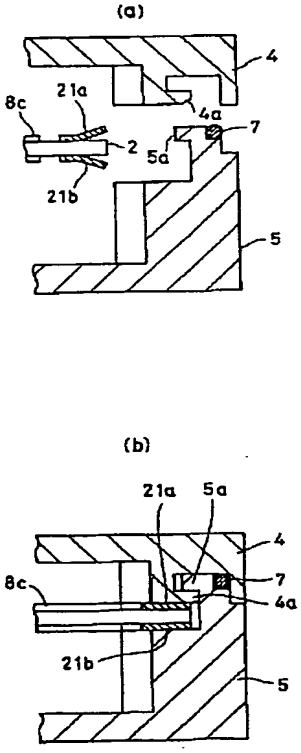
【図7】



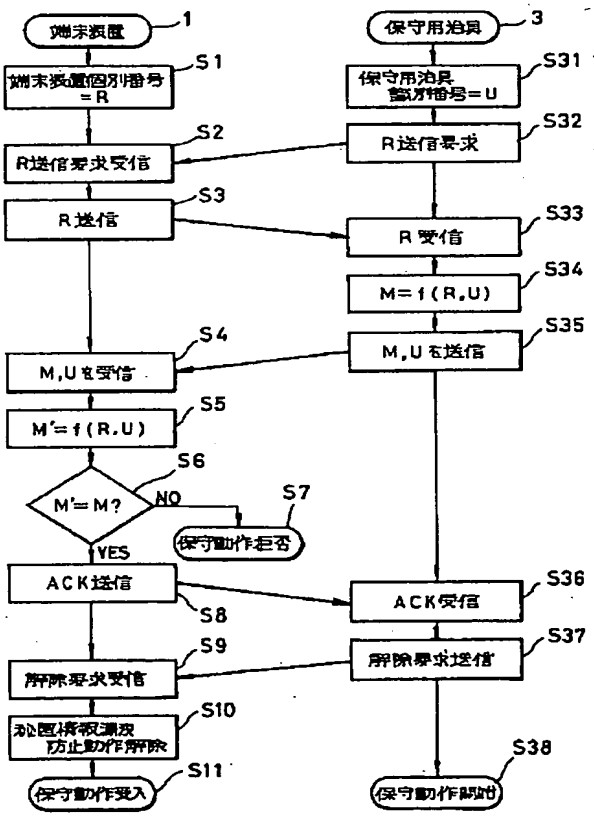
【図9】



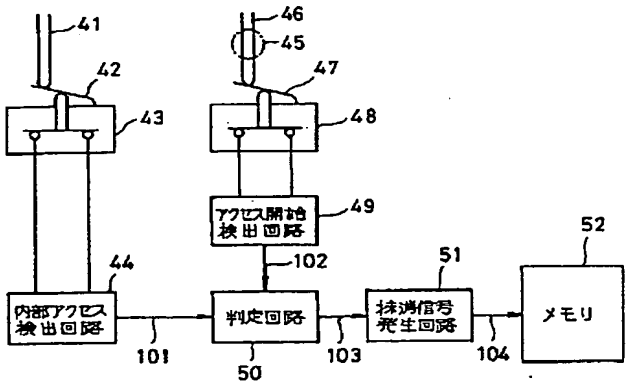
【図10】



【図11】



【図１２】


41
42
43
44
46
45
47
48
49
102
51
52
内部アクセス検出回路
判定回路
抹消信号発生回路
メモリ
101
50
103
104